CONCEPT OF OPERATIONS (CONOPS)

FOR

ADVANCED PROCESS AND TECHNOLOGY EXPERIMENT (APTX) 2001

28 September 2000

Prepared by: Lt Col Bob Pannone
Chief, Design Branch
AC2ISRC/AFEO

Reviewed by: Col Thompson, AC2ISRC/AFEO; Col Tillotson, ESC/CXE; Col Dunleavy, C2TIG; Lt Col Brundidge, ACC/SCN

Submitted by: Col Terry Thompson
Director, AFEO

Approved by: Maj Gen Gerald F. Perryman, Jr.
AC2ISRC/CC

OPR: AC2ISRC/AFEO
Langley AFB, VA 23665
DSN 575-2133

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Advanced Process and Technology Experiment (APTX) 2001 is one in a series of Air Force experiments that will help the US Air Force prepare for the challenges of the 21st Century Expeditionary Aerospace Force operations. To that end, the experiment attempts to anticipate and model a future command and control system. This model is based on the desired capabilities outlined in the Aerospace Command and Control & Intelligence, Surveillance and Reconnaissance Center (AC2ISRC) Campaign Plan End States and Objectives, as well as the Chairman of the Joint Chiefs of Staff objectives discussed in Joint Vision 2020.

The purpose of the APTX 2001 is to evaluate information sharing options that lead to meaningful collaboration in a US-led allied environment and serve as a risk reduction measure for the inclusion of allies in the Joint Expeditionary Force Experiment (JEFX) 2002. To achieve this purpose, APTX 2001 will explore solutions to overcoming impediments to collaboration that fall within the general areas of: (1) policy and standards (guidance), (2) processes, (3) data and networks systems, and (4) technology. Selected aspects of the intelligence function that are resident in a Combined Aerospace Operations Center (CAOC) will be used to evaluate the effectiveness of solutions to the impediments to effective allied collaboration.

APTX 2001 will use a North Atlantic Treaty Organization (NATO) setting as the backdrop for the experiment. The scenario will incorporate a "Framework Nation" effort with US leadership in which selected NATO allies are invited to participate in a CAOC. This setting leverages longstanding security agreements, simplifies experiment development, and helps maintain the experiment within resource limits. Specifically, APTX 2001 will examine selected processes and technologies associated with collaboration across security domains. It will also evaluate the automated reclassification and filtering of intelligence data derived from US strategic and theater sources, which is then transferred for use in a simulated “open floor” CAOC. Selected phases of the Joint Air Operations Planning Process will serve as the basic process for examining the technologies that support an "open floor" CAOC environment where alliance members share all filtered data and move about freely. To alleviate the problem of inadvertent release of US classified information, all individuals involved in this experiment will be appropriately cleared US citizens.

APTX 2001 will be conducted at the Combined Aerospace Operations Center Experimental (CAOC-X), Langley AFB, and the Joint C4ISR Battle Center (JBC) located at the Joint Training, Analysis, and Simulation Center (JTASC), Suffolk, VA, in the May 2001 time frame.

SECTION 1 - INTRODUCTION

1.1 PURPOSE.

The purpose of the Advanced Process and Technology Experiment (APTX) 2001 is twofold. First, it serves to evaluate information sharing options that lead to meaningful collaboration in a US-led allied environment. Second, it serves as a risk reduction measure for the inclusion of selected NATO allies in the Joint Expeditionary Force Experiment (JEFX) 2002.

1.2 RATIONALE.

1.2.1 The JEFX 99 After Action Report noted the exclusion of allied participants from many of the Combined Aerospace Operations Center (CAOC) functions due to information security requirements. In general terms, the final report recommended that the Air Force: (1) develop ways to integrate coalition partners into US experiments; (2) develop systems that are adaptable in a restricted access environment; and (3) commit to and develop a coalition-wide area network useable by all coalition forces.

1.2.2 Recommendations of the JEFX 99 report were researched for inclusion in JEFX 2000. The experimentation community studied options for allied participation that included the establishment of separate networks using firewalls in conjunction with security and control procedures. However, scheduling and funding required for network engineering and development of documentation for initiative compliance with national foreign disclosure policy precluded testing of a potential workable solution. APTX 2001 will build on the research of JEFX 2000 and the lessons learned from JEFX 99 to continue exploring processes and technologies for allied participation in CAOC operations. Although relatively small in terms of funding and manpower, APTX 2001 has the potential to significantly impact future coalition operations.

1.3 SCOPE.

1.3.1 APTX 2001 is a focused, small-scale, command and control experiment designed to explore processes and technologies for improving information sharing and collaboration among allies serving in a US led CAOC as a NATO-defined "Framework Nation" effort (see glossary). The experiment will serve as a risk-reduction effort to provide the Air Force leadership with a greater understanding of policy, process, system, and technology options required for improving allied information sharing during the much larger, follow-on JEFX 2002.

1.3.2 The discoveries of APTX 2001 should be scaleable in terms of worldwide applicability to US-led operations. However, time and funding constraints to support JEFX 2002 require that APTX 2001 leverage existing longstanding security agreements, which exist primarily among selected allies. As a result, APTX 2001 is designed primarily around an allied environment.

1.3.3 In exploring solutions to impediments for allied collaboration, APTX 2001 will examine the automated transfer of releasable US data to a simulated "open-floor" CAOC environment where alliance members share all filtered data and move about freely. Data (text, imagery, and track) from simulated and real-world strategic sources will be pushed and filtered using guard

technology to populate CAOC databases. US personnel, role-playing as allies, will then use the released data to perform selected CAOC Intelligence functions that currently support Air Tasking Order (ATO) development. In addition to automated data transfer, APTX 2001 will attempt to explore collaboration across security domains. The sufficiency of technology to support meaningful collaboration in the Intelligence processes will serve as the basis for assessment.

1.3.4 It is not within the scope of APTX 2001 to explore all aspects of information sharing within a fully operational CAOC. Resources limit APTX 2001 to exploring only a select portion of the total information flow. APTX 2001 will use the intelligence functions and processes resident in a notional combat theater to explore automated data flow of General Military Intelligence (GMI), imagery, and track data from the strategic/theater level to the operational level. The intelligence target development function of a US-led CAOC was selected as the process of choice because of data support requirements and the variation in type and sources of data.

SECTION 2 - DESCRIPTION

2.1 PROBLEM STATEMENT.

Information sharing between the United States and its allies is, sometimes, insufficient for effective command and control of allied combat aerospace operations. The incompatibility of database management systems, lack of common data standards, and the national foreign disclosure policies create conditions that inhibit efficient alliance collaboration in an information sharing environment and limit the timely, effective, and decisive application of combat aerospace forces.

2.2 APPROACH.

2.2.1 APTX 2001 will explore impediments to effective information sharing and meaningful collaboration that falls within the following general areas: (1) policy and standards (guidance), (2) processes, (3) data and networks systems, and (4) technology. Exploration begins during the initial concept development in which working groups, consisting of Air Force and DoD subject matter representatives, convene to formally quantify the current baseline situation. In addition, the subject matter experts will identify and refine a desired end-state and outline possible solutions to the impediments. The effectiveness of these solutions to enhance information sharing and collaboration will be the basis for the experiment.

2.2.2 For APTX 2001, the desired end-state is an alliance information environment that enables all CAOC personnel to effectively plan and prosecute aerospace operations. This end-state demands that information be shared in a truly “open-floor” environment with only the minimal input required from national enclaves. This desired end-state recognizes that allies will continue to require closed communication and maintain data that is restricted to nation-only use. As a result, national enclaves external to the “open floor” will continue to exist.

2.2.3 The desired end-state entails a restructuring and management of data within national enclaves so releasable information pertinent to a theater's operation is made available in an

"open-floor" setting. For APTX 2001, the "open-floor" setting is a US-led CAOC. Ideally, pertinent information will be pushed as quickly as possible to the "open-floor" CAOC via strategic and theater-level sources, and require little to no data from national enclaves for ATO development.

2.2.4 APTX 2001 will use a NATO setting as the backdrop for the experiment. This setting leverages longstanding security agreements, simplifies experiment development, and helps maintain the experiment within resource limits. Although exploration in APTX 2001 is expected to identify collaboration solutions that are applicable for CAOC employment worldwide, remaining within a NATO setting avoids the uncertainties associated with non-alliance coalitions and reduces the risk to APTX 2001 and thus, to JEFX 2002. It is anticipated that non-US personnel participation in JEFX 2002 will be limited to personnel from US allied countries, specifically selected NATO countries. Conducting APTX 2001 within a NATO setting will provide results for JEFX 2002 consideration. Using an alliance setting is an initial step toward addressing the more complex issues of information sharing in coalition operations.

2.2.5 APTX 2001 will use the Joint Air Operations Planning Process that leads to target development within a CAOC as the primary process for exploring solutions to the impediments for information sharing and collaboration. The experiment will not require a fully staffed CAOC for the experiment but will rely on a small cadre of intelligence specialists to satisfy processing requirements. Participants in the experiment will be limited to appropriately cleared US personnel only. Limiting participation to US personnel reduces the potential for inadvertent release of classified information during the development and execution phases of this security-centric experiment. Also, this limitation provides for greater experimentation flexibility for investigating options involving nondisclosure policy.

2.2.6 The interfaces between national intelligence sources and the CAOC will be at the Theater Joint Intelligence Center (JIC) level. The JIC will use reclassification processes and automated technologies to push data to a CAOC database repository. Through the reclassification processes and use of automation technologies, the amount of information pushed to the CAOC by the JIC is expected to be greater than that which is currently available.

2.2.7 APTX 2001 will use DOD information systems residing on JWICS and SIPRNET as data sources to populate US only systems in the simulated CINC JIC (at JBC) and simulated JTF JFACC (at JBC), respectively. This data will be subjected to national disclosure policy and transmitted through approved guards to populate the GMI, imagery and track databases in the CAOC (at Langley). The CAOC databases will be classified US SECRET REL NATO and available to all participants within the CAOC "open floor." The "open-floor" CAOC will be located at the Langley AFB Combined Aerospace Operations Center – Experimental (CAOC-X). Non-collateral and information not alliance releasable will be retained in the US SCI and SECRET enclaves located at the Joint C4ISR Battle Center (JBC), Suffolk, VA.

2.3. ASSUMPTIONS.

2.3.1 APTX 2001 is a risk reduction for JEFX 2002. NATO allies will participate in JEFX 2002. Therefore, APTX 2001 needs to address information sharing and meaningful collaboration as it pertains to NATO participation in a US-led CAOC environment.

2.3.2 TBMCS is the data management system.

2.3.3 Information required to be passed is sensitive in nature, i.e., classified at some level or provides insight into operations that should not be divulged to those without a need to know.

2.3.4 Alliance members are willing to share information with other participating members. However, nations are expected to maintain enclaves for nation-only collaboration and bilateral interaction.

2.3.5 APTX 2001 will operate within current security policy requirements. However, addressing security as it pertains to national disclosure policy is a fundamental area for exploration. Recommendations for modifying policy will be made as appropriate.

2.3.6 The "open-floor" CAOC concept will be employable worldwide and not limited to NATO. This means that the "open-floor" solution sets must be flexible enough to account for differences in alliance relationships.

2.3.7 The “open-floor” CAOC concept assumes the following:

2.3.7.1 All CAOC operations personnel will have access to information via TBMCS consistent with their role within the CAOC.

2.3.7.2 Controls to filter data, i.e. guards, will be external to the "open floor." This characteristic precludes the formation of security enclaves on the floor and supports the characteristic of equals on the "open floor." This characteristic reflects the need for open interaction between CAOC members to enhance information sharing and the effectiveness of collaboration. All guards will be employed in accordance with TOP SECRET/SCI and Below Interoperability (TSABI) and SECRET and Below Interoperability (SABI) DOD policy.

2.3.7.3 Classified data from US national organizations and ISR assets not assigned to the theater commander will be filtered by approved guard technology prior to release to the "open floor." This characteristic assumes that US national organizations will continue to maintain databases that preclude direct access by other than US members. This is also applicable to data link feeds from certain live assets. Data that is classified US only may be accessed from within a US-only enclave external to the "open floor."

2.3.7.4 The alliance organization will establish (agree to) a maximum-security level for information on the "open floor." All individuals with access to the floor will have a security clearance appropriate to the environment. This precludes escort requirements for assigned

members. The highest security level for the APTX 2001 "open-floor" CAOC is US SECRET REL NATO.

2.4 EXPERIMENT DESIGN.

2.4.1 The Joint Air Operations Planning Process will serve as the primary process for the exploration of collaboration within a US-led, "open-floor" CAOC environment. The JBC in Suffolk, VA will perform the functions of a CINC Joint Intelligence Center through which real world (e.g. DIA, NRO, NSA, etc.) and simulated source data is filtered through approved guard technology and pushed to the JTF JFACC and CAOC. The "open-floor" CAOC, replicated by the CAOC-X at Langley AFB, VA will receive the data for use in performing selected tasks involving intelligence preparation of the battlefield (IPB) and center of gravity assessment. The "open-floor" CAOC will consist of a planning cell type structure with approximately eight individuals. This cell will subscribe to released data residing in the CAOC databases and submits requests for information (RFI) to higher authority (i.e., JTF JFACC and CINC). In addition, the cell will be used to explore collaboration capability across security domains represented by the JBC (CINC JIC, JFACC) and CAOC-X.

2.4.2 Evaluation of the process and technologies used to overcome impediments to collaboration will involve, as a minimum, a comparison of data between two independent teams. One team (Team A) located at the JBC, will have access to all available US-source data. The other team (Team B) located at the CAOC-X, will have access to only filtered data. Using vignettes based on a NATO setting, the two teams will attempt to create areas of responsibility intelligence assessments that support notional JFACC guidance. The differences between the responsiveness and fidelity of the each team's consolidated findings; that is, the IPB assessments, course of action recommendations, target system selection, etc., will serve as a core part of the experiment evaluation.

2.5 SCHEDULE.

2.5.1 The Concept Development Conference (CDC) was held 9-10 May 2000. The call-for-initiatives advertisement in the “Commerce Business Daily” is planned for September 2000. The initial experiment conference (IEC) is scheduled for the December 2000/January 2001 time frame. There will be no spiral development conferences as traditionally held for the larger JEFXs. Work up for approved initiatives will be accomplished at the Command & Control Unified Battlespace Environment (CUBE), Hanscom AFB, MA, in the March 2001 time frame. APTX 2001 execution (to include set-up tear down time) is planned for May 2001 at the JBC in Suffolk, VA with a distributed site at the CAOC-X, Langley AFB, VA.

2.5.2 The JBC and/or ACC/SC will initiate Top Secret and Below (TSABI) and Secret and Below Interoperability (SABI) tickets to secure the assistance of the technical arms supporting those processes in implementing appropriate guards and developing acceptable rule sets.

2.6 FOREIGN DISCLOSURE:

A key lesson learned from JEFX 2000 is that obtaining disclosure authority for Secret NOFORN data is a complex process that involves mapping data flows, determining the owner of each type of data, and obtaining the permission of each data owner to disclose or release the data. Although data will not actually be released to foreign nationals during APTX 2001, a primary objective will be the construction of rule sets for guards that can be used in future contingencies or experiments; this requires that the process for obtaining disclosure authority be exercised. A secondary objective for APTX 2001 will be to obtain disclosure authority for all information passed across guards so that the guards can be used in JEFX 2002.

SECTION 3 – ADMINISTRATION.

3.1 Acronyms:

AIA	Air Intelligence Agency
AFEO	Air Force Experimentation Office
AOC	Aerospace Operations Center
AODB	Air Operations Data Base
APTX	Advanced Process and Technology Experiment
ATO	Air Tasking Order
CAOC	Combined Aerospace Operations Center
CAOC-X	Combined Aerospace Operations Center-Experimental
CIA	Central Intelligence Agency
C2	Command and Control
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CDC	Concept Development Conference
COG	Center of Gravity
CUBE	Command & Control Unified Battlespace Environment
DIA	Defense Intelligence Agency
DISN-LES	DISA Information Services Network-Leading Edge Services
DoD	Department of Defense
ESC	Electronic Systems Center
GMI	General Military Intelligence
IEC	Initial Experiment Conference
IPB	Intelligence Preparation of the Battlefield
ISR	Intelligence, Surveillance, and Reconnaissance
JIC	Joint Intelligence Center
JBC	Joint C4ISR Battle Center
JEFX	Joint Expeditionary Force Experiment
JSAF	Joint Semi-Automated Forces
JWICS	Joint Worldwide Information Communications System
MC	Millennium Challenge
MIDB	Modernized Integrated Database
NATO	North Atlantic Treaty Organization
NIC	National Intelligence Cell
NRO	National Reconnaissance Organization
NSA	National Security Agency
REL-NATO	Releasable to NATO
RFI	Request for Information
SABI	Secret and Below Interoperability
SIPRNET	Secure Internet Protocol Router Network
TBMCS	Theater Battle Management Core System

3.2 Glossary:

Framework Nation - Forces based on a Framework Nation are commanded by an officer of that nation, and the nation also provides the communications and logistic framework and leads on doctrinal matters. A significant proportion of the staff and the headquarters support will come from the framework nation; its working language is of that nation. Staff procedures, although based on Alliance standards, will also reflect those of the framework nation. In practice, however, once command and staff teams work together, procedures may incorporate the "best ideas" of the contributing nations. (AJP-01 [A])

Guard - A process (or set of controls) that mediates trusted transfers across security boundaries. Approved processes are normally implemented as rule sets in trusted computing systems acting as filters. Most guards support two-way data flow between systems operating at different security classification levels. Some guards support only high-to-low or low-to-high data flow. The general security requirements that guards must meet are: (1) Prevent leakage of data from the high to the low side, (2) Defend against penetration, and (3) Defend against denial-of-service or data integrity attacks from the low side.